REMARKS

Applicant has carefully reviewed and considered the Office Action mailed on 07/24/2009, and the references cited therewith.

Claims 34-36, and 40 are amended. Claims 1-33, 37-39, 41 and 42 are canceled. As a result, claims 34-36, 40, 43, and 44 are now pending in this application.

Information Disclosure Statement

Applicant submitted a Supplemental Information Disclosure Statement and a 1449 Form on 04/21/2005 and a Supplemental Information Disclosure Statement and a 1449 Form on 07/21/2005 and a Supplemental Information Disclosure Statement and a 1449 Form on 12/10/2007 and a Supplemental Information Disclosure Statement and a 1449 Form on 04/23/2008. Applicant respectfully requests that initialed copies of the 1449 Forms be returned to Applicants' Representatives thereby indicating that the cited references have been considered by the Examiner.

§101 Rejection of the Claims

Claims 34-36, 40 and 43-44 are rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Applicant submits that claims 40, 43, and 44 recite a computer, and therefore fall into the machine class of inventions under 35 U.S.C. §101. Thus, claims 40, 43, and 44 recite patentable subject matter. However, the Office Action asserts these claims are not patentable because they are "software per se." The Office Action also states claim 40's structure is entirely software. Applicant submits these assertions are unsupported by law and fact. Applicant submits there is no valid judicial precedent, statute, administrative law, or other legally binding rule holding that software *per se* is unpatentable in the United States. Furthermore, claim 40's structure is not necessarily exclusively software, as claim 40 recites "a processor." Given its broadest reasonable interpretation consistent with the specification, a processor can be hardware,

software, or a combination of hardware and software.[1] Therefore, Applicant submits that claims 40, 43, and 44 recite patentable processes under 35 U.S.C. §101.

According to the Federal Circuit's *en banc* holding in *In re Bilski*, 545 F.3d 943, 88 U.S.P.Q.2d 1385 (Fed. Cir. 2008), a claimed process is patentable if the process is tied to a particular machine or if the process transforms an article into a different state or thing. Claims 34-36 recite a process that is tied to two machines: a first server and a second server. Therefore, Applicant submits that claims 34-36 recite patentable processes under 35 U.S.C. §101.

§112 Rejection of the Claims

Claims 40 and 43-44 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Office Action asserts claim 40 is a "hybrid claim." The Office Action supports this position by arguing that claim 40's functional language moves it out of the apparatus class under 35 U.S.C. §101. MPEP §2173.05(p) states: "A functional limitation is an attempt to define something by what it does, rather than by what it is (e.g., as evidenced by its specific structure or specific ingredients). There is nothing inherently wrong with defining some part of an invention in functional terms. Functional language does not, in and of itself, render a claim improper. *In re Swinehart*, 439 F.2d 210, 169 USPQ 226 (CCPA 1971)." Therefore, Applicant submits claim 40, and its dependent claims, are patentable under 35 U.S.C. §101, and definite under 35 U.S.C. §112.

§103 Rejection of the Claims

Claims 34-36, 40 and 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,269,348 (hereinafter "Pare") in view of US Patent 6,332,193 (hereinafter "Glass").

Standard for Prima Facie Case of Obviousness

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d (BNA) 1596, 1598 (Fed. Cir. 1988). As discussed in *KSR International Co. v. Teleflex Inc. et al.* (U.S. 2007), the

[1] See MPEP §2111.

determination of obviousness under 35 U.S.C. § 103 is a legal conclusion based on factual evidence. See *Princeton Biochemicals, Inc. v. Beckman Coulter, Inc.*, 7, 1336-37 (Fed. Cir. 2005). The legal conclusion, that a claim is obvious within § 103(a), depends on at least four underlying factual issues set forth in *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17 (1966): (1) the scope and content of the prior art; (2) differences between the prior art and the claims at issue; (3) the level of ordinary skill in the pertinent art; and (4) evaluation of any relevant secondary considerations.

The test for obviousness under §103 must take into consideration the invention as a whole; that is, one must consider the particular problem solved by the combination of elements that define the invention. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir.1985). The Examiner must, as one of the inquiries pertinent to any obviousness inquiry under 35 U.S.C. §103, recognize and consider not only the similarities but also the critical differences between the claimed invention and the prior art. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990), reh'g denied, 1990 U.S. App. LEXIS 19971 (Fed. Cir.1990). Additionally, critical differences in the prior art must be recognized (when attempting to combine references). *Id.* Furthermore, when determining obviousness, the Examiner:

> must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of appellant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to "hindsight" based upon appellant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.[2]

[2] MPEP at § 2141.03.

Summary of Pare and Glass

Before discussing the rejections, this Response will summarize Pare and Glass.

Pare describes a system for authorizing credit and debit account transactions using biometric information instead of physical tokens, such as credit cards. Pare's point-of-sale system identifies a payer and payee. The system includes a party identification apparatus ("PIA") that receives a personal identification number ("PIN") and biometric information from the payer. The PIA sends the PIN and biometric information to a data processing center. Additionally, the PIA sends a PIA hardware identification code to the data processing center. The data processing center uses the PIN and biometric information to identify accounts associated with the payer, while using the PIA hardware identification code to identify an account associated with the payee. The PIA displays the accounts associated with the payer, and the payer selects an account from which to fund a purchase.[3] Thus, Pare's system verifies payers using biometric information, and verifies payees using PIA hardware identification codes.

Glass teaches a system for securely transmitting and authenticating biometric data over a network. Glass' system includes an authentication server, camera certification authority, and a client system (e.g., personal computer) connected to a camera. Glass' system restricts access to a secured resource, such as a webpage for transferring money over a network. Upon detecting a request to access the money transfer webpage, the authentication server sends a token (e.g., a random number) to the client system, which forwards the token to the camera. In turn, the camera accepts the token. The camera captures an image, and creates a secure image by creating a digital signature for the captured image. The digital signature is based on the image, token, and a secret key known to the camera. The camera sends the secure image to the client system, which in turn forwards the secure image to the authentication server. The authentication server checks whether the secure image has been modified by re-computing the digital signature (based on the token and secret key). Next, the authentication server verifies the biometric information, and grants access to the secure resource. Thus, Glass' system verifies users based on biometric information, a secret token, a secret key, and a digital signature.

[3] See Pare at column 15, line 20 *et seq.*

Discussion of the Rejected Claims

Applicant has amended claim 34 to recite the following:

> A computer-implemented method for verifying a user and a user computer comprising:
> receiving, at a first ~~mini-~~server, ~~at least one first mini-server~~ a first message from the user computer, the ~~at least one~~ first ~~mini-server~~ message including a first computer fingerprint file, ~~the first computer fingerprint file~~ identifying the user computer based on information associated with a plurality of components included in the user computer;
> comparing the first computer fingerprint file against a second computer fingerprint file to verify the user computer, the second computer fingerprint file including information associated with a plurality of components included in the user computer, and the second fingerprint file being accessible by the first ~~mini-~~server;
> receiving, at a second ~~mini-~~server, ~~at least one~~ a second ~~mini-server~~ message from the user computer, the ~~at least one~~ second ~~mini-server~~ message including ~~the~~ a first identification for the user, the first identification being associated with ~~based on~~ the first computer fingerprint file identifying the user computer; and
> comparing, at the second server, the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the second mini-server; and
> after the comparing of the first identification for the user against the second identification for the user to verify the user, generating a third ~~mini-server~~ message, at the second ~~mini-~~server, based upon the results of the comparison.

As shown, the computer-implemented method of claim 34 includes operations performed by two servers. The first server receives a computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer. The first server verifies the user computer by comparing the fingerprint file against another fingerprint file. As for the second server, it receives an identification associated with the user, where the identification is also associated with the fingerprint file. The second server verifies the user by comparing the user identification with another identification associated with the user.

In rejecting claim 34, the Office Action relies on Pare's passage at column 11, lines 39-45. More specifically, the Office Action asserts that Pare's passage teaches the first server's receiving and comparing operations. Pare's passage describes a Biometric-PIN Identification Subsystem (BPID) including a processor that receives a biometric sample and PIN, and

compares the biometric sample to registered biometric samples. If there is a match, the processor transmits an identity back to a transaction processor. If there is no match, the processor transmits a "party not identified" message back to the transaction processor.

Clearly, Pare's passage does not teach a first server receiving a computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer. It is also clear that Pare's passage does not teach the first server's comparing operation. Although the cited passage is off base, Pare does describe using a hardware security code to identify the party identification apparatus (PIA). According to Pare, and identification code is embedded, at manufacture time, in the PIA's write-once memory. As discussed above, Pare's system uses the code to identify a payee account. Therefore, Pare's use of hardware identifiers differs from claim 34's computer fingerprint file identifying a user computer based on information associated with a plurality of components included in the user computer.

In rejecting claim 34, the Office Action also relies on Glass' passage at column 10, lines 30-58. More specifically, the Office Action asserts that Glass' passage teaches claim 34's operations that are performed at the second server. According to the method of claim 34, the second server receives a user identification and compares the user identification to a stored user identification. In contrast, the passage from Glass describes a computer sending an image to a server, where the image was captured by a camera connected to the computer. Along with the image, the computer sends a digital signature and camera's unique serial number to the server. The digital signature and serial number are either embedded directly into the image or alongside the image in a data packet. The server sends the serial number to a central camera certification authority which looks-up the camera's public key and returns the public key to the server. Using a token (generated earlier) and the camera's public key, the server re-calculates the digital signature to ensure the image has not been tampered with. Applicant submits that Glass' complex image authentication process does not teach or suggest claim 34's operations for verifying user identification information.

As for claim 40, the Office Action has rejected claim 40 for the same reasons it rejected claim 34. As such, applicant submits that the cited passages do not teach or suggest the vendor computer system recited in claim 40.

Claims depending on claim 34 include all the elements recited in claim 34. Claims depending on claim 40 include all the elements recited in claim 40. As a result, applicant submits that claims depending on claim 34 or claim 40 are allowable for at least the same reasons discussed above, vis-à-vis claim 34.

Request for Telephone Interview

Applicant hereby requests a telephone interview with the Examiner before preparation of the next Office Action. Applicant requests the Examiner contact Andrew DeLizio (281-758-0025) to schedule an interview at the Examiner's convenience.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney Andrew DeLizio at 281-758-0025 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-3998.

Respectfully submitted,

DeLizio Gilliam, PLLC
15201 Mason Road
Suite 1000-312
Cypress, TX 77433
281-758-0025

Date 11/24/2009 By /Andrew DeLizio Reg. 52,806/
Andrew DeLizio
Reg. No. 52,806